



Privacy Act 103

Safeguarding Privacy Data



Why You Are Being Asked to Take this Training Now

- In a number of recent incidents, personal data has been lost, stolen, or compromised.
- The Office of Management and Budget, the Federal entity responsible for overseeing the Privacy Act, has mandated that the Federal workforce complete annual Privacy training.
- Don't let YOU or a member of your staff be the next accused of carelessly handling Privacy Act data!





Safeguarding Requirements

- Three Levels of Safeguards are Required for handling Privacy data:
 - Technical
 - Physical
 - Administrative
- These individuals are responsible for installing safeguards:
 - Technical: Information Technology Staff
 - Physical: Your Security or Public Safety Office
 - Administrative:
 - Privacy Act System Managers
 - Local Privacy Act Officials
 - Supervisors
- These individuals are responsible for following rules for safeguarding:
 - You!





Marking Privacy Data

- Privacy Act data is to be handled as “For Official Use Only” (FOUO).
- Mark Privacy data with a handling notice when it is created or received:
 - **“For Official Use Only-Privacy Act of 1974”**; or
 - **“For Official Use Only-Privacy Sensitive”**
- Place the FOUO marks at the top and bottom of each page or screen.
- Before disseminating Privacy data, make sure it carries the FOUO handling notice. Use DLA Form 1880, Privacy Act Cover Sheet, to safeguard records containing Privacy Act protected data from unauthorized disclosure.





Transporting Privacy Data

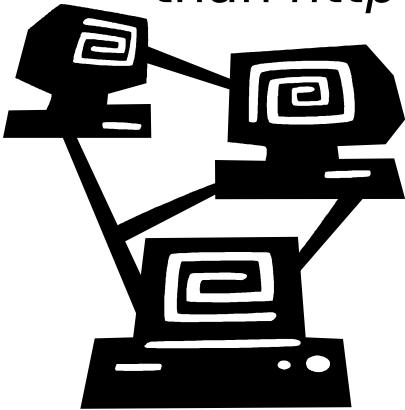


- Via Ground Mail:
 - Use kraft / white envelopes. NEVER use “holey joes” or messenger-type envelopes.
 - Double wrap using an inner and outer envelope if you deem it appropriate. DLA Form 1461, Privacy Act Safeguard Label, can be used on the inner envelope to indicate safeguards are necessary to protect the data within.
 - Mark the envelope to the attention of an authorized recipient.
 - Never indicate on the outer envelope that it contains Privacy Data.
- Handcarrying:
 - Use DLA Form 1880, Privacy Act Cover Sheet, to safeguard records containing Privacy Act protected data from unauthorized disclosure. This form may be ordered through your Forms Manager.
 - Use DLA Form 22, For Official Use Only Cover Sheet, to safeguard all other FOUO types of information from unauthorized disclosure. This form may be ordered through your Forms Manager.



Transporting Privacy Data (cont'd)

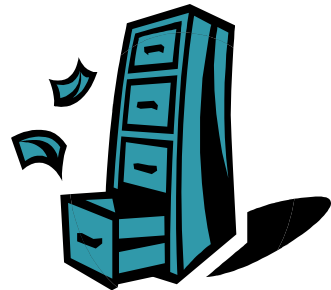
- Via E-mail:
 - Use Common Access Card procedures
 - Announce in the subject line and the opening line of text that you are relaying FOUO material.
- Via the Internet
 - Use Secure Socket Layer (SSL) connections. NOTE: URLs that require an SSL connection start with *https* rather than *http*.





Storing Privacy Data

- Duty Hours
 - Cover or place in an out-of-sight location when those not authorized access to the data enter the work space.
 - Use filtering devices on computer screens to blacken the view.
 - Lock computers when leaving – even for brief periods.
- After Duty Hours
 - If the building is locked or manned by security, place records in locked or unlocked drawer or cabinet.
 - Special categories of Privacy data should be placed in locked receptacles.

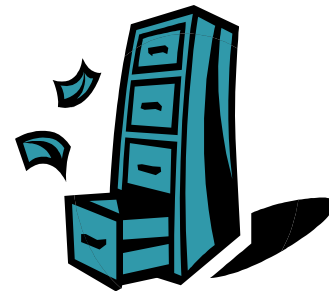




Storing Privacy Data (cont'd)

What are Some Special Categories of Privacy Data?

- Investigative Files
- Personnel Files
- Security Clearance Files
- EEO Files
- Adverse Action Files
- Any category that, if released, would embarrass or harm the subject.





Disposing of Privacy Data

- Use any means that prevents inadvertent compromise. A disposal method is considered adequate if it renders the information unrecognizable or beyond reconstruction.
- Disposal methods may include:
 - Tearing
 - Burning
 - Melting
 - Chemical decomposition
 - Pulping
 - Pulverizing
 - Shredding
 - Mutilation





Sharing Privacy Act Data

- Follow the “need-to-know” principle. Share only with those specific DoD employees who need the data to perform official, assigned duties.
- If the Privacy Act System Manager has granted you authority to make disclosures outside DoD:
 - Share only with those individuals and entities outside DoD that are listed in the “Routine Use” clause of the governing Privacy Act system notice.
- If you have doubts about sharing data, consult with your supervisor, the Privacy Act system manager, or your local Privacy Act Officer.





Information for Teleworkers

- Paper Records:
 - Place Privacy Act data in locked drawers, locked briefcases, or other secure areas where family or household members cannot access it.
- Electronic Records:
 - Use password protection protocols and encryption. Share your password with no one.

REMINDER: Do not remove FOUO data from the worksite without pre-approval from your supervisor. Ensure the FOUO data is secured via password protection and encryption.



Reporting Unauthorized Disclosures

In some instances, management may have to notify affected parties of lost, stolen, or compromised data. If you learn of inappropriate disclosures:

- Immediately notify your supervisor, your local Privacy Act Officer, and the Privacy Act System Manager of the occurrence.
- For World Wide Web postings, make a note of where the information was posted by copying the Uniform Resource Locator (URL). The URL is the address listed at the top of the screen. Most URLs begin **http://www**. For example, DLA's home page URL is **http://www.dla.mil**.



Criminal Penalties for Noncompliance with the Privacy Act

- For knowingly and willfully disclosing Privacy Act data to any person not entitled to access:
 - Misdemeanor criminal charge, and a fine of up to \$5000 (for each offense).
- For maintaining a System of Records without meeting the public notice requirements:
 - Misdemeanor criminal charge, and a fine of up to \$5000 (for each offense).
- For knowingly and willfully requesting or obtaining records under false pretenses:
 - Misdemeanor criminal charge, and a fine of up to \$5000 (for each offense).





Civil Penalties for Noncompliance with the Privacy Act

- The Privacy Act also imposes civil penalties when an employee:
 - Unlawfully refuses to amend a record.
 - Unlawfully refuses to grant access to records.
 - Fails to maintain accurate, relevant, timely and complete data.
 - Fails to comply with any Privacy Act provision or agency rule that results in an adverse effect.
- Penalties include:
 - Payment of actual damages.
 - Payment of reasonable attorney's fees.
 - Adverse personnel action, including removal from employment.
- Civil penalties apply to Federal agencies, not employees. If you violate an individual's privacy, the individual can only sue the government. But the government can prosecute YOU!





If You Have Access to Privacy Data .

- Protect it at all times.
- Do not share it with anyone unless
 - The recipient is listed in Section (b) of the Privacy Act or
 - The record subject has given you written permission to disclose it.
- Password-protect and encrypt personal data placed on shared drives, the Internet or the Intranet.
 - Issue passwords only to those with a clear need for access.
 - Remove it once it no longer needs to be posted.
 - Never post Privacy data to E-Workplace or Outlook.
- Constantly monitor your actions: If I do this, will I increase the risk of unauthorized access?

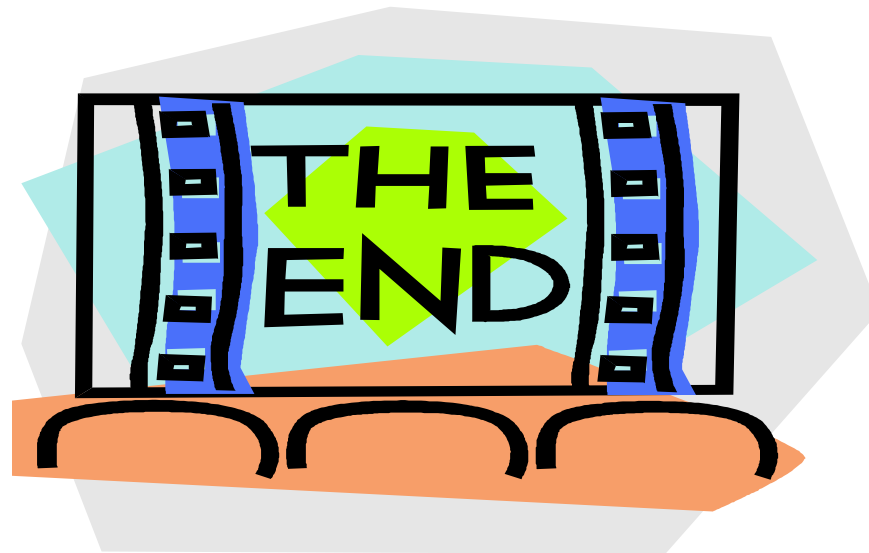


Remember:
You may be subject to penalties for
violating the Privacy Act.



More Tips for Avoiding Privacy Breaches

- Take privacy protection seriously.
- Know the Privacy Act requirements.
- Respect the privacy of others.
- Alert your supervisor or other management officials when you see personal data left unattended.



Thank you for completing this important training!



For More Information, Contact:



Jody Sinkler
DLA HQ Privacy Officer
Headquarters Defense Logistics Agency
703-767-5045
jody.sinkler@dla.mil

OR

Kathy Tennessee
DLA FOIA & Privacy Specialist
Headquarters Defense Logistics Agency
703-767-6183
Kathy.tennessee@dla.mil

DEFENSE LOGISTICS AGENCY

AMERICA'S COMBAT LOGISTICS SUPPORT AGENCY



WARFIGHTER SUPPORT ENHANCEMENT

STEWARDSHIP EXCELLENCE

WORKFORCE DEVELOPMENT